REMARKS

The courtesy extended to the undersigned attorney for applicant during an interview on November 22, 2005, by Assistant Examiner Elahee and Primary Examiner Escalante is noted.

During the interview, Examiner Elahee provided attorney for applicant with a copy of the provisional application on which Okamoto et al., (US Publication No. 2004-0128257) is based. The provisional application has a date of March 29, 2000, that antedates applicants' priority date of June 17, 2000. The issue concerning the provisional application is moot, however, as a result of arguments advanced with regard to the rejection of claims rejected in the office action on the Okamoto et al. reference.

During the interview, attorney for applicant indicated claim 28 would be amended for clarity, as set forth in the present amendment. The amendment to claim 28 does not require consideration of new issues or a new search because claim 40, as previously submitted, required a control arrangement that is responsive to the location-match subsystem detecting a location match to cause the mobile entity to pass the service token to the service delivery subsystem. The Examiners agreed entry of the amendment is permissible.

The examiners also agreed the arguments, as set forth in this amendment, are persuasive. As a result, the application will either be allowed, or a new, non-final action will be issued, based on a new search.

During the interview, attorney for applicant explained the subject matter of claims 1 and 18 in simplified form, and referred specifically to the example set forth in the specification as filed on page 14, lines 6-11. Of course, the passage on page 14, lines 6-11 is merely exemplary. Attorney for applicant also described the subject matter of claims 28 and 40, in connection with

the embodiment of Figure 9 and the description thereof in the application as filed, at page 17, line 7-page 18, line 14.

Applicants offer the following comments with regard to the various rejections set forth in the office action.

Independent claims 1 and 18 (claim set 1) are concerned with a situation where, after a user is qualified to receive a particular service, a *user-associated instance of an executable program* for implementing the service is stored either in a user mobile entity or in a service system: Data indicative of a triggering location is also stored. Subsequently, the executable program is executed to provide the service when the user arrives at the triggering location. The *executable program is customized to a transaction* in respect of which the service is to be delivered.

Independent claims 1 and 18 are not obvious due to Valentine (US 6,011,973) in view of Tarbox (US 5,705, 798).

Valentine simply discloses enabling or disabling a cell phone depending on its location.

In one embodiment, data relating to allowed areas of operation of the phone is stored in memory 150 of the phone. The phone has a location device 130 (e.g. a GPS receiver) which a controller 120 uses to determine when the phone is in an area where operation is authorized, as indicated by the data stored in memory 150; when in such an area, controller 120 enables operation of the phone.

In a second embodiment, the phone location determined by device 130 is sent to a mobile phone infrastructure for comparison with stored location data indicative of where operation of the phone is authorized. If the phone is in an authorized area of operation, the infrastructure returns an authorization signal to enable phone operation.

A user can subscribe to have the cell phone operate in one or more telephone service areas 200, 210 (see column 4) which implies that the data indicating the authorized areas of operation is stored on a subscriber basis.

A feature of Claims 1 and 18 that is not disclosed by Valentine is:

"conducting a transaction ..... and after the transaction has been conducted storing:

.....

- **a user-associated instance of an executable program for implementing said particular service, the program instance being customized for said transaction and distinct from the location data,"**

Tarbox discloses a financial transaction card that stores small programs for controlling the interaction of an ATM with a user. Each program relates to a specific type of transaction. The user pre-selects what programs are stored on the card. The customer may also specify parameters of the programs – for example, for the "Quick Cash" transaction, the user specifies the amount to be retrieved with this program.

Applicant can not agree it is obvious to combine Valentine and Tarbox to provide a user-associated instance of executable program for implementing the particular service, the program being customized to the transaction and being location triggered. The motivation for doing this is allegedly "in order to conduct one or more electronic transaction of product without having any operating difficulties".

Controlling the operation of a mobile phone by location is not in the same technical field, or a related technical field, to electronic transaction cards.

It is highly unlikely that anyone would want to make an electronic transaction of the type discussed by Tarbox, location triggered.

In claims 1 and 18, the "particular service" is provided as a consequence of an earlier transaction; the service is not itself the transaction. It is not at all clear what the examiner has in mind as to the result of combining Valentine and Tarbox. At the interview, the examiners were unable to identify what, in the proposed combination of Valentine and Tarbox, is the "transaction" of claim 1, and what is the "particular service" of claim 1.

Independent claims 28 and 40 are related to the situation where, after a user being qualified to receive a particular service, *a service token is stored in a user mobile entity*; data indicative of a triggering location is also stored. Subsequently, in response to the triggering location being reached, *the token is passed to a service provider* system so the system can provide the particular service. At the service system a *check is made as to whether the token originates* from a party for whom the service system is willing to provide service delivery (the party from whom the token originates being the party carrying out qualification of the user).

The examiners agreed the rejection of independent claims 28 and 40 of Claim Set 2 as being obvious due to Valentine (US 6,011,973) in view of Okamoto (US 2004/0128257) is wrong. Claims 28 and 40 require storage of location data indicative of where a particular service is to be provided. In Valentine, when a user subscribes to a mobile phone operator, location data is stored. The location data indicates where operation of a mobile phone is to be inhibited, which applicants agree indirectly indicates where operation is to be allowed.

Claims 28 and 40 require a service token to be stored in the mobile entity identifying the service to be provided. In the first embodiment of Valentine, the location data is stored in the mobile entity; this location data indicates where operation of the mobile entity or of "a requested

service or capability" is prohibited (see col.1, line 66). This implies that some sort of service indicator may be stored in the mobile entity.

Claims 28 and 40 indicated that in response to the mobile entity reaching a location indicated by the location data, the service token is sent to a service provider system. In Valentine, only in the second embodiment is data sent from the cell phone. This data is the current location of the cell phone and not a service token or service indicator. In Valentine's first embodiment, wherein a service indicator may be stored by the mobile entity, this service indicator is not sent to a service provider system but is used by the mobile entity itself.

Claims 28 and 40 require the service system to use a "qualifying party indicator," included in the service token, to check that the party which qualified the user as entitled to receive the service, is a party for which it is willing to provide service delivery. This, of course, is not done by Valentine.

While the first embodiment of Valentine appears to be closest to Claim 28 because it discloses the possibility of storing a service indicator in the mobile entity, the service indicator in the first embodiment is not passed to a service system and does not include a "qualifying party indicator" that is used by the service system to check that the party which qualified the user as entitled to receive the service, is a party for whom it is willing to provide service delivery

The Okamoto reference is somewhat confusing but basically concerns a system in which a user can contact a ticket service system (TSS) and, with the involvement of a secure transaction service system (STSS), obtain a ticket for an event or service, wherein the ticket includes various items of information including 'secure contents'.

There appear to be two possible ways of interpreting the disclosure of Okamoto as being applicable to claims 28 and 40.

(1) The user "ticket" can be considered similar to the "service token" of claim 28; in this case, the "particular service" of claim 28 would be the service for which the ticket has been obtained.

(2) Alternatively, the "confirmation token" can be considered similar to the "service token" of claim 28. In the Figure 7 embodiment of Okamoto, a confirmation token is provided by the ticket service system 704 to the user system 700. System 700 passes the confirmation ticket to the secure transaction service system 702 to obtain the desired ticket. Before issuing the ticket the secure transaction service system contacts the ticket service system to receive information about the transaction in respect of which the ticket is to be issued. It is not clear whether the "particular service" of claim 28 would be the service for which the ticket is being obtained, or the service of issuing the ticket that is carried out by the secure transaction service system.

The examiner has used both the "ticket" and "confirmation token" in his arguments without distinguishing between them.

Thus, considering the passage in the Action at page 11, lines 3 to 11, where the examiner argues Okamoto discloses "a service token ... including a service identifier identifying said particular service"; the specific references given by the examiner (paragraphs 0108, 0139, 0142) all relate to the confirmation token. However, in the following passage in the Action (page 11, lines 12 to 18), where the examiner argues Okamoto discloses a qualifying party identifier, the specific references in the Office Action relate to (1) information contained in a ticket (paragraph

0119) and (2) information apparently associated with a confirmation token (paragraphs 0139, 0142).

Although Okamoto discloses an identifier of the ticket service system in information put into a ticket (paragraph 0119), there is no disclosure of a check being made by the ticket verifier system 206 (Figure 2, paragraphs 0098, 0099) or 502 (Figure 5, paragraph 0105) that the ticket has been issued by a ticket service system or the service provider system is willing to provide the service concerned. Instead, the purpose of the ticket verifier system is "to read the ticket information and, in some embodiments, to contact the STSS 20 to verify the validity of ticket 208"; no details are given about this validity check.

It is very difficult to see how the examiner can justify combining Valentine and Okamoto. As already indicated, the first embodiment of Valentine arguably discloses a service indicator stored in the mobile entity. The examiner is relying on this in his arguments (see page 11, lines 19, 20). However, this service indicator is used locally and in a negative sense to disable operation. When operation is enabled, there will, of course, be a check made by the mobile phone infrastructure of Valentine that the mobile phone is an authorized phone but that has nothing at all to do with the service indicator stored by the phone.

There is no reason why the service indicator implicitly stored by the first embodiment of Valentine would:

- be sent from the phone to a service system (the service system would be run by the operator who already knows where the mobile phone is and is not allowed to operate);
- include an indicator of the operator (the relevant operator is inherently the one providing the mobile phone services to the mobile phone).

It is very difficult to see what Okamoto can add to any argument based on Valentine. It can be argued that Valentine effectively stores on the mobile phone, information about where a particular service is available; this service is then brought to life when the mobile phone is appropriately located. However, the authorization check that the operator carries out prior to providing any mobile phone with service is based on the identity of the mobile phone and on data held by the operator in its own databases – the operator would not be looking to receive a service indicator from the mobile entity as this would result in a much more complicated system.

It must also be remembered that Valentine's objective is to prevent mobile phone operation in areas either where phone operation could be dangerous (runway areas) or are outside its operating area.

Based on the foregoing, it was agreed at the interview that independent claims 1 and 18 are not rendered obvious by the combination of Valentine and Tarbox and that independent claims 28 and 40 are not rendered obvious by Valentine and Okamoto. Consequently, all claims dependent on independent claims 1, 18, 28 and 40 are patentable over the combinations of Valentine and Tarbox; Valentine and Okamoto; Valentine, Tarbox and Okamoto; Valentine, Tarbox and Suzuki; Valentine in view of Tarbox, Suzuki and Okamoto and Valentine in view of Suzuki and Eldridge, as well as Valentine in view of Okamoto and Norris. The references that have not been discussed do not cure the above-noted deficiencies in the references specifically relied on to reject the independent claims.

The office action alleges the "qualifying-party indicator" introduced into claim 28 is not disclosed in the description nor is its use in checking that the service token originates from that party.

In response, the "qualifying-party indicator" is formed by the "certificate "disclosed on page 17, line 19 of the description. The term "certificate" is used in relation to a digital signature signed by the service factory. Lines 24 to 27 explain that the service system can:

"check that the service token originates from a service factory for which it is willing to provide service delivery (this check involves checking the identity of the signing party with the certification authority in standard manner)"

A person of ordinary skill in the art of digital signatures would fully understand that:

- the digital signing of the service token by the service factory would be done using a private key, the corresponding public key being included in the "certificate";

- the certificate would be issued by the certification authority and associates the public key of the service factory with the identity of the service factory;

- the certificate would be signed by the certification authority.

The service system can check the authenticity of the certificate by using the public key of the certification authority. Thereafter, the service system can check that the service token has been signed by the party identified in the certificate by using the public key in the certificate.

The description is not explicit about certain features of the digital signing process because such a process is so well known. A good tutorial on the web is given by the American Bar Association at http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html, copy enclosed. The tutorial demonstrates that the techniques of digital signatures and certificates are now so widespread that we do not need to turn to "a person of ordinary skill in the art".

Based on the foregoing, the examiners agreed at the interview there is an adequate basis in the specification for the claim 28 requirement for the "qualifying-party indicator."

Application No. 09/881,040 Docket No. 30003033-2 (1509-188)

In view of the foregoing amendments and remarks, withdrawal of the final rejection and allowance are in order.

The Examiner is invited to telephone the undersigned, Applicant's attorney of record, to facilitate advancement of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025 and please credit any excess fees to such deposit account.

Respectfully submitted,

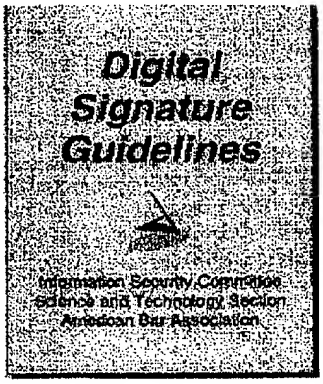
Colin I'ANSON et al.

Alan M. Lowe

Alian M. Lowe
Registration No. 19,641

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400
Telephone: 703-684-1111
Facsimile: 970-898-0640
Date: November 23, 2005
AML/tal

Science & Technology Home
E-Commerce and IT Division
Life & Physical Sciences Division
Standing & Special Committees
National Conference of Lawyers & Scientist
The SciTech Lawyer Editorial Board
The SciTech Lawyer
e-BLAST
Jurimetrics
Publications
Calendar of Events
Sites of Interest
About the Section
Contact Us
Join the Section



American Bar Association
Section of Science and Technology
Information Security Committee

Digital Signature Guidelines Tutorial

Tutorial

In today's commercial environment, establishing a framework for the authenticat of computer-based information requires a familiarity with concepts and professio skills from both the legal and computer security fields. Combining these two disc is not an easy task. Concepts from the information security field often correspon loosely to concepts from the legal field, even in situations where the terminology similar. For example, from the information security point of view, "digital signatur means the result of applying to specific information certain specific technical pro described below. The historical legal concept of "signature" is broader. It recogni any mark made with the intention of authenticating the marked document. <2> Ir digital setting, today's broad legal concept of "signature" may well include markir diverse as digitized images of paper signatures, typed notations such as "/s/ Joh Smith," or even addressing notations, such as electronic mail origination header

From an information security viewpoint, these simple "electronic signatures" are from the "digital signatures" described in this tutorial and in the technical literatur although "digital signature" is sometimes used to mean any form of computer- ba signature. These Guidelines use "digital signature" only as it is used in informatic security terminology, as meaning the result of applying the technical processes described in this tutorial.

To explain the value of digital signatures in legal applications, this tutorial begins an overview of the legal significance of signatures. It then sets forth the basics o signature technology, and examines how, with some legal and institutional infrastructure, digital signature technology can be applied as a robust computer-l alternative to traditional signatures.

Signatures and the Law

A signature is not part of the substance of a transaction, but rather of its represe or form. Signing writings serve the following general purposes:<3>

- **Evidence:** A signature authenticates a writing by identifying the signer wi signed document. When the signer makes a mark in a distinctive manner, writing becomes attributable to the signer.<4>
- **Ceremony:** The act of signing a document calls to the signer's attention t significance of the signer's act, and thereby helps prevent "inconsiderate engagements.<5>
- **Approval:** In certain contexts defined by law or custom, a signature expr the signer's approval or authorization of the writing, or the signer's intentic it have legal effect.<6>
- **Efficiency and logistics:** A signature on a written document often impart sense of clarity and finality to the transaction and may lessen the subseq need to inquire beyond the face of a document.<7> Negotiable instrumen example, rely upon formal requirements, including a signature, for their at change hands with ease, rapidity, and minimal interruption.<8>

The formal requirements for legal transactions, including the need for signatures in different legal systems, and also vary with the passage of time. There is also variance in the legal consequences of failure to cast the transaction in a requirec The statute of frauds of the common law tradition, for example, does not render transaction invalid for lack of a "writing signed by the party to be charged," but re makes it unenforceable in court,<9> a distinction which has caused the practical application of the statute to be greatly limited in case law.

During this century, most legal systems have reduced formal requirements,<10> least have minimized the consequences of failure to satisfy formal requirements. Nevertheless, sound practice still calls for transactions to be formalized in a man which assures the parties of their validity and enforceability.<11> In current prac formalization usually involves documenting the transaction on paper and signing authenticating the paper. Traditional methods, however, are undergoing fundam change. Documents continue to be written on paper, but sometimes merely to sa the need for a legally recognized form. In many instances, the information excha effect a transaction never takes paper form. Computer-based information can al utilized differently than its paper counterpart. For example, computers can "read" information and transform the information or take programmable actions based c information. Information stored as bits rather than as atoms of ink and paper can near the speed of light, may be duplicated without limit and with insignificant cos

Although the basic nature of transactions has not changed, the law has only beg adapt to advances in technology. The legal and business communities must dev rules and practices which use new technology to achieve and surpass the effect historically expected from paper forms.

To achieve the basic purposes of signatures outlined above, a signature must ha following attributes:<12>

- **Signer authentication:** A signature should indicate who signed a docum message or record,<13> and should be difficult for another person to proc without authorization.
- **Document authentication:** <14> A signature should identify what is sign <15> making it impracticable to falsify or alter either the signed matter or t signature without detection.

Signer authentication and document authentication are tools used to exclude impersonators and forgers and are essential ingredients of what is often called a "nonrepudiation service" in the terminology of the information security professior

nonrepudiation service provides assurance of the origin or delivery of data in ord protect the sender against false denial by the recipient that the data has been re or to protect the recipient against false denial by the sender that the data has be sent. <16> Thus, a nonrepudiation service provides evidence to prevent a perso unilaterally modifying or terminating legal obligations arising out of a transaction effected by computer-based means. <17>

- **Affirmative act:** The affixing of the signature should be an affirmative act serves the ceremonial and approval functions of a signature and establish sense of having legally consummated a transaction.
- **Efficiency:** Optimally, a signature and its creation and verification proces should provide the greatest possible assurance of both signer authenticity document authentic, with the least possible expenditure of resources.

Digital signature technology generally surpasses paper technology in all these attributes. <18> To understand why, one must first understand how digital signat technology works.

How Digital Signature Technology Works

Digital signatures are created and verified by cryptography, the branch of applie mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use what is known as "pub cryptography," which employs an algorithm using two different but mathematicall related "keys;" one for creating a digital signature or transforming data into a see unintelligible form, and another key for verifying a digital signature or returning th message to its original form. <19> Computer equipment and software utilizing tw keys are often collectively termed an "asymmetric cryptosystem."

The complementary keys of an asymmetric cryptosystem for digital signatures ai arbitrarily termed the private key, which is known only to the signer <20> and us create the digital signature, and the public key, which is ordinarily more widely kn and is used by a relying party to verify the digital signature. If many people need verify the signer's digital signatures, the public key must be available or distribut of them, perhaps by publication in an on-line repository or directory where it is ea accessible. Although the keys <21> of the pair are mathematically related, if the asymmetric cryptosystem has been designed and implemented securely <22> it "computationally infeasible <23> to derive the private key from knowledge of the key. Thus, although many people may know the public key of a given signer and to verify that signer's signatures, they cannot discover that signer's private key a it to forge digital signatures. This is sometimes referred to as the principle of "irreversibility."

Another fundamental process, termed a "hash function," is used in both creating verifying a digital signature. A hash function is an algorithm which creates a digit representation or "fingerprint" in the form of a "hash value" or "hash result" of a standard length which is usually much smaller than the message but neverthele substantially unique to it. <24> Any change to the message invariably produces different hash result when the same hash function is used. In the case of a secu function, sometimes termed a "one-way hash function," it is computationally infe <25> to derive the original message from knowledge of its hash value. Hash fun therefore enable the software for creating digital signatures to operate on smalle predictable amounts of data, while still providing robust evidentiary correlation to original message content, thereby efficiently providing assurance that there has no modification of the message since it was digitally signed.

Thus, use of digital signatures usually involves two processes, one performed by signer and the other by the receiver of the digital signature:

- **Digital signature creation** uses a hash result derived from and unique tc the signed message and a given private key. For the hash result to be sei there must be only a negligible possibility that the same digital signature c be created by the combination of any other message or private key.
- **Digital signature verification** is the process of checking the digital signa reference to the original message and a given public key, thereby determi whether the digital signa ture was created for that same message using tl private key that corresponds to the referenced public key.

To sign a document or any other item of information, the signer first delimits prec the borders of what is to be signed. The delimited information to be signed is ter the "message" in these Guidelines. Then a hash function in the signer's software computes a hash result unique (for all practical purposes) to the message. The s software then transforms the hash result into a digital signature using the signer' private key. <26> The resulting digital signature is thus unique to both the messa the private key used to create it.

Typically, a digital signature (a digitally signed hash result of the message) is att to its message and stored or transmitted with its message. However, it may also sent or stored as a separate data element, so long as it maintains a reliable assc with its message. Since a digital signature is unique to its message, it is useless wholly disassociated from its message.

Verification of a digital signature is accomplished by computing a new hash resu original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier check whether the digital signature was created using the corresponding private key; a whether the newly computed hash result matches the original hash result which transformed into the digital signature during the signing process. The verification software will confirm the digital signature as "verified" if: (1) the signer's private k used to digitally sign the message, which is known to be the case if the signer's p key was used to verify the signature because the signer's public key will verify o digital signature created with the signer's private key; <27> and (2) the message unaltered, which is known to be the case if the hash result computed by the verif identical to the hash result extracted from the digital signature during the verifica process.

Various asymmetric cryptosystems create and verify digital signatures using diff algorithms and procedures, but share this overall operational pattern.

The processes of creating a digital signature and verifying it accomplish the esse effects desired of a signature for many legal purposes:

- **Signer authentication:** If a public and private key pair is associated with identified signer, the digital signature attributes the message to the signer digital signature cannot be forged, unless the signer loses control of the p key (a "compromise" of the private key), such as by divulging it or losing t media or device in which it is contained.
- Message authentication: The digital signature also identifies the signed message, typically with far greater certainty and precision than paper sigr Verification reveals any tampering, since the comparison of the hash resu made at signing and the other made at verifying) shows whether the mes the same as when signed.
- **Affirmative act:** Creating a digital signature requires the signer to use the signer's private key. This act can perform the "ceremonial" function of ale the signer to the fact that the signer is consummating a transaction with le consequences. <28>
- **Efficiency:** The processes of creating and verifying a digital signature pro

high level of assurance that the digital signature is genuinely the signer's. the case of modern electronic data interchange ("EDI") the creation and verification processes are capable of complete automation (sometimes re to as "machinable"), with human interaction required on an exception bas Compared to paper methods such as checking specimen signature cards methods so tedious and labor-intensive that they are rarely actually used practice -- digital signatures yield a high degree of assurance without add greatly to the resources required for processing.

The processes used for digital signatures have undergone thorough technologic review for over a decade. Digital signatures have been accepted in several natio International standards developed in cooperation with and accepted by many corporations, banks, and government agencies. <29> The likelihood of malfuncti security problem in a digital signature cryptosystem designed and implemented prescribed in the industry standards is extremely remote, <30> and is far less th risk of undetected forgery or alteration on paper or of using other less secure ele signature techniques.

Public Key Certificates

To verify a digital signature, the verifier must have access to the signer's public k have assurance that it corresponds to the signer's private key. However, a public private key pair has no intrinsic association with any person; it is simply a pair of numbers. Some convincing strategy is necessary to reliably associate a particul person or entity to the key pair.

In a transaction involving only two parties, each party can simply communicate (l relatively secure "out-of-band" channel such as a courier or a secure voice telep the public key of the key pair each party will use. Such an identification strategy small task, especially when the parties are geographically distant from each othe normally conduct communication over a convenient but insecure channel such a Internet, are not natural persons but rather corporations or similar artificial entitie act through agents whose authority must be ascertained. As electronic commerc increasingly moves from a bilateral setting to the many-on-many architecture of t World Wide Web on the Internet, where significant transactions will occur among strangers who have no prior contractual relationship and will never deal with eac again, the problem of authentication/nonrepudiation becomes not merely one of efficiency, but also of reliability. An open system of communication such as the I needs a system of identity authentication to handle this scenario.

To that end, a prospective signer might issue a public statement, such as: "Signa verifiable by the following public key are mine." However, others doing business the signer may for good reason be unwilling to accept the statement, especially there is no prior contract establishing the legal effect of that published statement certainty. A party relying upon such an unsupported published statement in an o system would run a great risk of trusting a phantom or an imposter, or of attempt disprove a false denial of a digital signature ("nonrepudiation") if a transaction sh turn out to prove disadvantageous for the purported signer.

The solution to these problems is the use of one or more trusted third parties to associate an identified signer with a specific public key. <31> That trusted third p referred to as a "certification authority" in most technical standards and in these Guidelines.

To associate a key pair with a prospective signer, a certification authority issues certificate, an electronic record which lists a public key as the "subject" of the cer and confirms that the prospective signer identified in the certificate holds the corresponding private key. The prospective signer is termed the "subscriber. <32

certificate's principal function is to bind a key pair with a particular subscriber. A "recipient" of the certificate desiring to rely upon a digital signature created by th subscriber named in the certificate (whereupon the recipient becomes a "relying can use the public key listed in the certificate to verify that the digital signature w created with the corresponding private key. <33> If such verification is successfu chain of reasoning provides assurance that the corresponding private key is hel subscriber named in the certificate, and that the digital signature was created by particular subscriber.

To assure both message and identity authenticity of the certificate, the certificati authority digitally signs it. The issuing certification authority's digital signature on certificate can be verified by using the public key of the certification authority liste another certificate by another certificate authority (which may but need not be or higher level in a hierarchy) <34>, and that other certificate can in turn be authent by the public key listed in yet another certificate, and so on, until the person relyi the digital signature is adequately assured of its genuineness. In each case, the certification authority must digitally sign its own certificate during the operational of the other certificate used to verify the certification authority's digital signature.

A digital signature, whether created by a subscriber to authenticate a message c certification authority to authenticate its certificate (in effect a specialized messa should be reliably time-stamped to allow the verifier to determine reliably whethe digital signature was created during the "operational period" stated in the certific which is a condition upon verifiability of a digital signature under these Guideline

To make a public key and its identification with a specific subscriber readily avail use in verification, the certificate may be published in a repository or made avail other means. Repositories are on-line databases of certificates and other inform available for retrieval and use in verifying digital signatures. Retrieval can be accomplished automatically by having the verification program directly inquire of repository to obtain certificates as needed.

Once issued, a certificate may prove to be unreliable, such as in situations when subscriber misrepresents his identity to the certification authority. In other situati certificate may be reliable enough when issued but come to be unreliable someti thereafter. If the subscriber loses control of the private key ("compromise" of the key), the certificate has become unreliable, and the certification authority (either without the subscriber's request depending on the circumstances) may suspend (temporarily invalidate) or revoke (permanently invalidate) the certificate. Immed upon suspending or revoking a certificate, the certification authority must publish of the revocation or suspension or notify persons who inquire or who are known received a digital signature verifiable by reference to the unreliable certificate.

Challenges and Opportunities

The prospect of fully implementing digital signatures in general commerce prese both benefits and costs. The costs consist mainly of:

- **Institutional overhead:** The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring in the performance of their functions.
- **Subscriber and Relying Party Costs:** A digital signer will require softwa will probably have to pay a certification authority some price to issue a ce Hardware to secure the subscriber's private key may also be advisable. P relying on digital signatures will incur expenses for verification software a perhaps for access to certificates and certificate revocation lists (CRL) in repository.

On the plus side, the principal advantage to be gained is more reliable authentic messages. Digital signatures, if properly implemented and utilized offer promisin solutions to the problems of:

- **Imposters**, by minimizing the risk of dealing with imposters or persons wh attempt to escape responsibility by claiming to have been impersonated;
- **Message integrity**, by minimizing the risk of undetected message tampe and forgery, and of false claims that a message was altered after it was s
- **Formal legal requirements**, by strengthening the view that legal require of form, such as writing, signature, and an original document, are satisfie digital signatures are functionally on a par with, or superior to paper forms
- **Open systems**, by retaining a high degree of information security, even f information sent over open, insecure, but inexpensive and widely used ch

Contact Information:
Section of Science & Technology Law
321 N. Clark St.
Chicago, IL, 60610
phone: (312) 988-5599
sciencetech@abanet.org